

MAKING A FAIR ROULETTE FROM A POSSIBLY BIASED COIN

Edsger W. DIJKSTRA

Department of Computer Sciences, The University of Texas at Austin, Austin, TX 78712-1188, USA

Communicated by J. Misra

Received 27 November 1989

Revised 19 June 1990

Keywords: Random numbers, probability, gambling

We are given a possibly biased coin, i.e., a coin that, when flipped, shows head or tail with the probabilities p and q respectively, with $p + q = 1$, but not necessarily $p = q$. We don't know the values of p and q , we only know that the coin remains "the same", i.e., that p and q are constant in time. The problem is to design an experiment with 37 different outcomes of equal probability.

In a variable B of type "sequence of 37 faces", we record 37 successive flippings of the coin; if all the faces in B are the same, we start afresh, otherwise we accept the value of B . This first stage of the design has been inspired by (i) the consideration that the experiment has to fail (to terminate) if the coin is so extremely biased that one of the faces *never* shows up, and (ii) the fact that $2^{37} - 2$ is a multiple of 37. (One of Fermat's theorems states that for prime p , $n^p - n$ is divisible by p .)

With B thus determined, we consider the 37 sequences obtained by rotating (to the left, say) for $0 \leq k < 37$ the sequence B over k positions. Because B is not periodic with period 1 and 37 is prime, these 37 sequences are all different. Moreover, since they all contain the same number of heads (and the same number of tails), they are 37

equally likely B -values. To complete our design, we have to introduce a convention that establishes a 1-1 correspondence between those 37 sequences and the numbers from 0 through 36. We can, for instance, associate with B the number of positions B has to be rotated over so as to yield the lexical minimum of those 37 sequences. (With 37 replaced by 2, the above yields a well-known method for making a fair coin from a possibly biased one [0].)

Remark. In the above analysis it is irrelevant that the given coin has only 2 faces; with a possibly loaded die, one can proceed in exactly the same manner. Essential use has been made of the primality of 37, but the generalization to a composite number is not difficult: we can make a fair die out of a fair binary roulette and a fair ternary roulette.

Reference

- [0] J. von Neumann, Various techniques used in connection with random digits (Summary written by George E. Forsyth), in: *John von Neumann, Collected Works, Vol. V* (Pergamon, Oxford, 1963) 768-770.